The Commonwealth of Massachusetts

AUDITOR OF THE COMMONWEALTH

ONE ASHBURTON PLACE, ROOM 1819

BOSTON, MASSACHUSETTS 02108

TEL. (617) 727-6200

A. JOSEPH DeNUCCI

AUDITOR

No. 2001-0004-4C

INDEPENDENT STATE AUDITOR'S
REPORT ON THE EXAMINATION OF
INFORMATION TECHNOLOGY-RELATED CONTROLS AT THE
EXECUTIVE OFFICE OF ELDER AFFAIRS

July 1, 2000 to November 30, 2001

OFFICIAL AUDIT REPORT

FEBRUARY 28, 2002

2001-0004-4C

TABLE OF CONTENTS

INTRODUCTION

The Executive Office of Elder Affairs (EOEA) is authorized under Chapter 19A of the Massachusetts General Laws and is under the supervision and control of the Secretary of the Executive Office of Elder Affairs. The EOEA's primary mission is to promote the dignity, independence, and rights of Massachusetts elders and to support their families through advocacy and the development and management of programs and services.

The Office consists of four operational divisions - the Office of Finance and Administration, the Office of Program Management, the Office of Policy Development, and the Office of the Secretary. The EOEA has approximately 86 employees and volunteers, and in fiscal year 2001, the EOEA had a budget of $169,154,789 to support 96 elder affairs programs. During fiscal year 2001, the EOEA responded to over 14 thousand complaints from senior citizens of the Commonwealth.

The EOEA relies on IT resources located at its offices and at the Commonwealth's Information Technology Division's (ITD) data center in Chelsea to assist in carrying out its mission and programs by providing IT processing support. All computer equipment under EOEA's immediate charge is located in its administrative offices. The Office also uses statewide application systems that are operated from ITD's Chelsea data center. The IT configuration at EOEA's offices includes a local area network (LAN), comprised of six file servers and approximately 90 desktop workstations. Operating systems for the common area workstations are Windows NT, Windows 95, and Windows 2000. The principal application systems used by EOEA to support its business processes are the Home Care Management Information System (HOMIS), National Aging Program Information System (NAPIS), and Ombudsman.

HOMIS primarily resides on workstations networked to third-party elder service provider vendors, known as Aging Services Access Points or Area Agencies on Aging. An individual vendor can be an Aging Services Access Point or an Area Agency on Aging or both. HOMIS, which operates using a FOXPRO database, is not networked to the University of Massachusetts Medical Center (UMass Medical), which administers the application. HOMIS-related financial and statistical information, which is entered by intake workers and case managers, is transmitted or forwarded to the EOEA through e-mail and in hard-copy form. EOEA, in turn, forwards the information to UMass Medical where it is summarized and then sent back to EOEA for a final review. Using this information, the EOEA will then submit a HOMIS report to its federal oversight agency, the Administration On Aging (AOA).

The NAPIS application resides on workstations networked through three vendors that are independent Area Agencies on Aging. NAPIS also operates using a FOXPRO database and is not networked to UMASS Medical, which administers the application. NAPIS financial and statistical information is

entered by intake workers and case managers. The information is then sent to the EOEA using e-mail and in hard-copy form. The EOEA then sends the information to UMass Medical where it is compiled and sent back to EOEA for a final review. Using this information EOEA then submits a State Program Report to its federal oversight agency AOA.

The Ombudsman application captures information regarding complaints that are brought forward from or regarding clients in long-term care facilities. After the information has been entered into the system, it is forwarded on disks and by hard copy to the EOEA. The data entered into the Ombudsman system does not include client names or confidential information.

The EOEA is currently working on the Elder Affairs Systems Environment (EASE) project with UMASS Medical. EASE will replace HOMIS, NAPIS and Ombudsman as EOEA's only application system to be used in conjunction with its service-provider vendors.

AUDIT SCOPE, OBJECTIVES, AND METHODOLOGY

Audit Scope

We performed an information technology (IT) audit at the Executive Office of Elder Affairs (EOEA) for the period of July 1, 2000 through November 30, 2001. The scope of the audit, which was conducted from April 6, 2001 to November 30, 2001, consisted of an examination of internal controls over selected information technology functions and an analysis of vendor satisfaction with EOEA's various automated systems that assist the vendors in tracking and reporting services provided. We evaluated IT-related controls pertaining to organization and management, physical security, environmental protection, hardware and software inventory, system access security, business continuity planning and on-site and off-site storage of magnetic media. In addition, we reviewed selected reporting requirements of EOEA.

Audit Objectives

The primary objective of our audit was to determine whether adequate controls were in place and in effect for EOEA's IT processing environment with respect to IT resource management, system access security, and availability of automated processing. With respect to IT-related controls, we sought to determine whether adequate general controls were in effect to support a properly controlled processing environment.

We sought to determine whether controls regarding physical security and environmental protection were in place and in effect to safeguard computer operations and IT-related assets. Our objective with respect to hardware and software inventory was to determine whether IT-related assets were properly accounted for and reported to the Office of the State Comptroller (OSC) as part of the entity's Generally Accepted Accounting Principles (GAAP) report.

We sought to determine whether adequate internal controls were in place to provide reasonable assurance that only authorized users could access EOEA's automated systems. Regarding availability of processing capabilities and electronic data, our objective was to determine whether adequate business continuity plans were in place to provide reasonable assurance that mission-critical and essential computer operations could be regained within an acceptable period of time should a disaster render computer systems inoperable or inaccessible. In conjunction with reviewing business continuity planning, we also sought to determine whether proper backup procedures were being performed and whether copies of backup magnetic media were being stored in secure on-site and off-site locations.

With respect to the user satisfaction analysis, we solicited information as to whether EOEA's principal application systems adequately met user (vendor) needs.

Audit Methodology

To determine the scope of the audit, we performed pre-audit survey work regarding EOEA's IT environment. The pre-audit work included interviews with senior management; a review of policies, procedures, and other internal control documentation; and observation of IT-related areas. To obtain an understanding of the Office's activities and internal control environment, our pre-audit work included a review of EOEA's mission, organizational structure, and primary business functions. We assessed the strengths and weaknesses of the internal control system for selected IT activities. Upon completion of our pre-audit work, we determined the scope and objectives of the audit.

To obtain an understanding of the type of data and the form of the data elements contained in EOEA's database, we obtained and reviewed file descriptions and record layouts of the data files. We requested and received a list of all files that comprised the EOEA's database. After obtaining an understanding of the stated or documented contents of the data files, we obtained hardcopy reports processed by EOEA.

To determine whether IT-related assets were adequately safeguarded, we reviewed physical security and environmental protection over the microcomputer systems and online workstations through observation, interviews with EOEA management and staff, and completion of appropriate audit checklists. We also requested hardware and software inventories and tested the inventories received for accuracy.

To obtain an understanding of and evaluate the organization and management of IT operations, we reviewed the Office's organizational structure with respect to IT operations and evaluated reporting lines, span of control, job descriptions, and separation of duties. We reviewed IT policies and procedures regarding system access security to determine the level of documentation and appropriateness of control procedures related to our audit work.

To assess the adequacy of business continuity planning, we reviewed the adequacy of formal planning that would be used to restore computer operations in the event that the mainframes or microcomputer systems were damaged or destroyed. We interviewed EOEA management to determine whether the criticality of application systems had been assessed, whether risks and exposures to computer operations had been evaluated, and whether a written business continuity plan was in place. The interview also addressed an evaluation of the adequacy of controls to ensure that data files and software would be available should the automated systems be rendered inoperable, including the adequacy of provisions for on-site and off-site storage of critical backup tapes. We also interviewed EOEA management responsible for creating backup copies of computer-related media.

We reviewed EOEA's system access security policies and procedures to prevent and detect unauthorized access to the EOEA data files and software installed on ITD's mainframe. A step-by-step examination was performed to see how EOEA system users log onto the three computer systems: HOMIS, NAPIS, and Ombudsman and what security controls these systems have in effect.

To review user satisfaction with EOEA's three computer systems, HOMIS, NAPIS, and Ombudsman, the auditors conducted nine site visits to vendors and conducted interviews using a user satisfaction survey. In addition, we reviewed policies and procedures and system documentation maintained by vendors, as well as user manuals for the three systems.

Our audit was conducted in accordance with Generally Accepted Government Auditing Standards (GAGAS) of the United States and generally accepted auditing practices. Audit criteria used in the audit included management policies and procedures, and control guidelines outlined in *Control Objectives for Information and Related Technology* (CobiT) as issued by the Information Systems Audit and Control Association, July 2000. CobiT control objectives and management control practices were developed as a generally applicable and accepted standard for sound information technology security and control practices, providing a reference framework for management, users, security practitioners, and auditors.

AUDIT SUMMARY

Based on the results of our audit, we found that internal controls in place at the Executive Office of Elder Affairs (EOEA) provided reasonable assurance that controls over physical security and environmental protection would be met. However, our audit detected areas in need of strengthening in regard to the safeguarding and proper accounting of IT-related equipment inventory. There was no software inventory and the hardware inventory was incomplete. Auditors obtained purchase orders of hardware items not on the hardware inventory that appeared to have been purchased within the past two years. The hardware inventory had not been updated due to inadequate IT staffing. We noted that, by the end of the audit, the hardware inventory had been updated. Another area in need of improvement was software inventory control in that the EOEA did not have a software inventory record. At the close of our audit this issue remained unresolved. With respect to business continuity planning, EOEA had not developed a disaster recovery plan, and while on-site storage of magnetic media had been provided, there was no provision for the proper storage of off-site magnetic media. With respect to reporting requirements, we obtained General Accepted Accounting Principles (GAAP reports), which were submitted Office of the Comptroller, for the last two fiscal years. EOEA was unable to provide the fiscal year 2000 State Program. Report. This report was not submitted as required to the Federal Administration on Aging. Site visits were made to nine EOEA vendors throughout the state. During these site visits, user satisfaction surveys were conducted to obtain the level of satisfaction of intake workers and management who use EOEA's three application systems, HOMIS, NAPIS, and Ombudsman. Through these site visits, It was determined that users were reasonable satisfied with the 3 systems. It was further determined that a reasonable level of system access security controls were in place to ensure only authorized users have access to the systems.

AUDIT RESULTS

1. Inventory Control of IT Resources

At the time of our audit, the EOEA maintained a fixed-assets inventory record to account for property and equipment under their charge. With respect to IT resources, we initially found that the inventory records did not identify all computer equipment installed at EOEA and did not include the cost of IT resources for all items listed. In addition, we found that no information was recorded to identify software residing on EOEA systems. Based on interviews with EOEA staff, it appeared that the hardware items not included had been purchased within a two-year period and that the fixed-asset inventory record had not been updated, ostensibly due to inadequate IT staffing.

Due to the lack of complete hardware and software inventory records, the EOEA was unable to adequately account for all IT resources. The absence of a complete software inventory record inhibits the EOEA's ability to account for software, make decisions regarding software allocation and use, and detect unauthorized or illegal copies of software. By having an up-to-date complete hardware and software inventory record, EOEA can better support IT configuration management.

Although EOEA did not have a significant number of software products installed on its systems, maintaining a record of software addresses accounting and operational control objectives. Because of the absence of software records, management could not properly account for all copies of software installed on its file servers, on-line workstations, and laptops or determine whether only authorized software was residing on these systems or whether software had been properly allocated. In addition, the absence of a software inventory record precluded an accounting of the total number of software copies allowed under certain license agreements and inhibited the office from having an accurate accounting of software inventory costs.

Sound management practices and generally accepted industry standards advocate that a perpetual inventory be maintained for all property and equipment, including hardware and software, and that sufficient policies and procedures be in effect to ensure the integrity of the inventory record. Further, in accordance with Massachusetts General Laws Chapter 7, Subsection 4A, each state agency is required to record and to report on state-owned assets to certain control agencies, such as the Office of the State Comptroller (OSC). Tests of software inventory against purchase records and software installation enables organizations to detect misplaced, lost, missing, unauthorized, or illegal copies of software.

Chapter 647 of the Acts of 1989 states, in part, that . . . "The agency head shall be responsible for maintaining accountability for the custody and use of resources and shall assign qualified individuals for that purpose, and periodic comparison should be made between the resources and the recorded accountability of the resources to reduce the risk of unauthorized use or loss and protect against waste and

wrongful acts." Moreover, the OSC's "Internal Control Guide for Departments" promulgated under Chapter 647 of the Acts of 1989, requires that "fixed assets be accounted for per existing regulations, that they be safeguarded to ensure that they are being used as intended, and that a property officer be designated to provide control of inventories."

The OSC requires that state departments and agencies properly account for all fixed-asset transactions, including the proper recording and reconciliation of Generally Accepted Accounting Principles (GAAP) Fixed Assets. GAAP Fixed Assets are defined as all land, regardless of cost, and buildings and equipment with a useful life of one year or more, and an original cost of $15,000 or more. GAAP Fixed Assets also include computer software, with a useful life of one year or more, and an original cost of $15,000 or more. According to the OSC, all GAAP Fixed Assets must be recorded at the time of acquisition in the MMARS Fixed Asset Subsystem. In addition, the OSC requires that the physical reconciliation of all property and equipment be completed as of June 30th of each fiscal year.

The OSC's MMARS Fixed Asset Subsystem User Guide states "all assets entered into the MMARS Fixed Asset Subsystem must be recorded onto the system within seven days of acquisition." Further, the OSC requires that "all acquired assets entered into the Fixed Asset Subsystem be verified by the department that the information entered into the system is correct and appropriate for that particular asset." The initial entry of a fixed-asset record should be verified to the supporting documentation within three days of the asset being recorded into the system. The OSC also requires that the fixed-asset inventory be reconciled at least annually to the books and records maintained by the department, either on the MMARS Fixed Asset Subsystem or other documented methods.

During our audit, issues brought to EOEA's attention regarding the inventory of IT resources were addressed for computer equipment. We noted that computer equipment was completely retagged with EOEA identification numbers and that the fixed assets inventory record was updated to reflect information for IT resources not previously included. At the close of our field work, we completed additional audit tests, which verified that IT resources had been tagged and properly recorded on EOEA's inventory system-of-record.

Recommendation:

The EOEA should expand the use of its fixed-asset inventory record to include all software, system utilities, and any other software products. The Office should develop documented policies and procedures for maintaining a software inventory record. The established procedures should include identifying required data fields related to software inventory control, procedures to capture information regarding bundled software, and procedures for reconciliation of the software inventory record to procurement records, software installed and deleted software.

Auditee's Response:

> *The Executive Office of Elder Affairs has reviewed the draft audit report and concurs with the recommendations . . . . The Agency has begun its software inventory and expects to complete this within the next three to four months.*

Auditor's Reply:

We concur with the Office 's effort to establish a software inventory record within the next three to four months. The software inventory records should reconcile to, or be a part of, the Office's overall fixed-asset inventory record and include all software, system utilities, and any other software products. In conjunction with developing a software inventory, the Office should develop documented policies and procedures for maintaining the software inventory record. We will review the policies and procedures for the software inventory record, as well as the inventory system of record for software and hardware during our next audit.

2. Business Continuity Planning

We determined that the EOEA did not have a formal tested, disaster recovery and business continuity plan to provide for the timely restoration of mission-critical and important business functions should automated systems be rendered inoperable.

At the start of the audit, we found that EOEA did maintain backup tapes for applications and data on an open shelf within the file server room, however there were no backup tapes maintained off-site. Subsequently, backup tapes were kept off-site at the MIS Director's home, contrary to sound backup procedures.

The absence of a formal, tested, disaster recovery and business continuity plan, which designates an alternate processing site and includes off-site storage of backup data tapes, places at risk the Office's ability to regain mission-critical and essential data processing operations within an acceptable time period.

Without a comprehensive, formal, and tested disaster recovery and business continuity plan, including required user area plans and off-site storage of data tapes, critical and essential information related to the Office's clients and programs may be unavailable should the automated system be rendered inoperable.

The objective of business continuity planning is to help ensure the continuation of mission-critical and essential functions should a disaster cause significant disruption to computer operations. Business continuity planning for information services is part of business continuity planning for the entire organization. Generally accepted practices and industry standards for computer operations support the

need for each entity to have an ongoing business continuity planning process that assesses the relative criticality of information systems and develops appropriate contingency and recovery plans, if required. To that end, the entity should assess the extent to which it is dependent upon the continued availability of information systems for all required processing or operational needs and develop its recovery plans based on the critical requirements of its information systems.

The success of the business continuity planning process requires management commitment. Senior management and system users should be closely involved in business continuity planning to help ensure that there is a clear understanding of the entity's information system environment, that determinations of system criticality and the risks and exposures associated with the systems are correct, that appropriate data processing and user area plans are developed based on the relative criticality and importance of systems, and that adequate resources are available.

Recommendation:

The EOEA should establish procedures to ensure that the relative importance, or criticality, of its systems is evaluated on an annual basis, or upon major changes to user requirements. The Office should also conduct a formal risk analysis of its IT components on an annual basis, or upon major changes to the relevant IT infrastructure. Based on the results of the risk analysis and criticality assessment, EOEA should confirm its understanding of business continuity requirements and amend recovery plans, if necessary, to address mission-critical and essential IT-supported business functions.

The EOEA should ensure that the disaster recovery and business continuity plan provides recovery strategies with respect to all potential disaster scenarios. The recovery plan should contain all pertinent information needed to effectively and efficiently recover critical operations within the needed time frames. In addition, the Office should ensure that appropriate user area plans are in place and sufficiently understood by management and staff to enable business areas to continue their operations should automated processing be lost for an extended period of time also, off-site storage of backup media should be included in the plan. The plans should take into account unavailable processing due to a loss of file servers, or LAN- or microcomputer-based system operations.

We recommend that the business continuity plan identify alternate sites for business operations and data processing. We further recommend that the disaster recovery and business continuity plan be tested and formally reviewed and approved. The plan should be periodically reviewed and updated when necessary to ensure that it remains appropriate to recovery needs. The EOEA should ensure that management and staff are adequately trained in the execution of the plan. The completed plan should be distributed to appropriate management and staff members, and a copy should be stored in a secure off-site location.

Auditee's Response:

> *The Executive Office of Elder Affairs has reviewed the draft audit report and concurs with the recommendations . . . . The Agency has begun work on these issues . . . . A business continuity plan, including an offsite storage location for the Office's backup server, will be completed within the next six months.*

Auditor's Reply:

Although we concur with the Office 's intent to develop a business continuity plan within the next six months, including an off-site storage location for the Office's backup server, we recommend that procedures be established to provide for off-site storage of backup media as soon as possible. The final, tested disaster recovery and business continuity plan should provide recovery strategies with respect to a range of potential disaster scenarios. The business continuity plan would take into account the possibility of unavailable processing due to the loss of critical IT resources, such as the file servers, or the loss of LAN- or microcomputer-based system operations. Importantly, the plan will need to be tested and formally reviewed and approved. The completed plan should be distributed to appropriate management and staff members, and a copy should be stored in a secure off-site location. We will review the completed and tested disaster recovery and business continuity plan at our next audit.

3. Filing of the Fiscal Year 2000 State Program Report

In the course of our audit, we determined that EOEA had not submitted a federal grant-related report to its federal oversight agency providing details on the level of services provided to the elderly in the Commonwealth for fiscal year 2000. According to EOEA, the report, which is required to be submitted to the Administration On Aging (AOA), was not prepared due to the absence of a previously outsourced computer consultant. As a result, the EOEA had not filed its fiscal year 2000 and 2001 State Program Report to the AOA.

Under Title 3 and Title 7 of The Older Americans Act of 1965, state agencies on aging are required to submit fiscal-year reports to the AOA. The reports contain financial and statistical client data pertaining to services provided to the elderly. Submission of the reports on a timely basis will address the federal reporting requirement and provide necessary information on elderly services to the federal oversight agency. Although EOEA may not be at risk of potential penalties from the AOA, submission of required reports will eliminate any potential risk of penalties in the future from the AOA. Subsequent to our field work, it is our understanding that EOEA will be working in concert with the University of Massachusetts Medical Center to attain the necessary technical assistance to compile reports required to be submitted to the AOA.

Federal grant expenditures at EOEA were $27 million in fiscal year 2000 and $27 million in fiscal year 2001.

Recommendation:

We recommend that the EOEA continue to work with the University of Massachusetts Medical Center to ensure timely submission of reports required to be filed annually with the AOA to meet reporting requirements of the federal Older Americans Act of 1965.

Auditee's Response:

> *The Executive Office of Elder Affairs has reviewed the draft audit report and concurs with the recommendations . . . . The Agency has begun work on these issues . . . The NAPIS Reports will be submitted more timely in the future.*

Auditor's Reply:

We concur with the Office 's submitting of the NAPIS Reports in a timelier manner. Hopefully, the use of the University of Massachusetts Medical Center to expedite the processing of report-related data will prove to be beneficial. Also, the upgrade of the data-collection software will hopefully assist in speedier report processing. We will review procedures for the submittal of the NAPIS Reports during our next audit.